# Beyond GnuPG and Tor

## Technologies to secure the future Internet

Jeff Burdges & Christian Grothoff

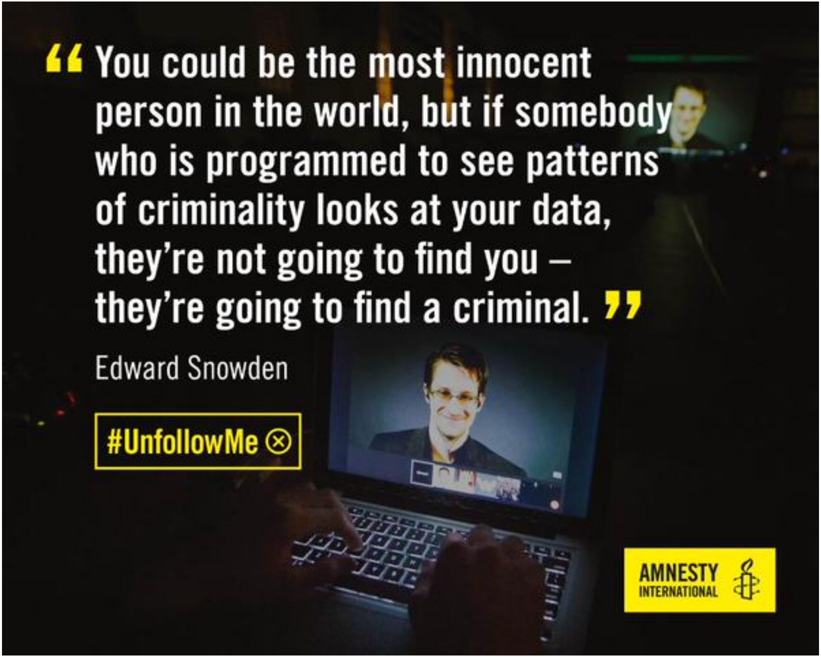
28.6.2015

**Encryption is not enough.**

*"We've developed a machine learning algorithm that is able to predict which customers will leave your site without purchasing any of your products .. and the capability to offer only this group a steeper discount than normal to entice them to purchase before leaving,"*

*—Freshplum.*

Amazon? Airline sites?



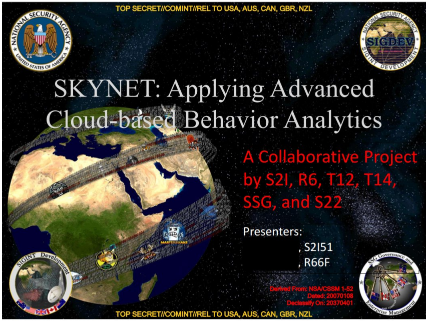
“You could be the most innocent person in the world, but if somebody who is programmed to see patterns of criminality looks at your data, they’re not going to find you – they’re going to find a criminal.”

Edward Snowden

#UnfollowMe ⊗

AMNESTY INTERNATIONAL

Former CIA agent Jeffrey Stirling was convicted of sharing classified information with the New York Times reporter James Risen based solely upon the fact that they spoke over the phone many times.



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

SKYNET: Applying Advanced Cloud-based Behavior Analytics

A Collaborative Project by S2I, R6, T12, T14, SSG, and S22

Presenters:
[redacted], S2I51
, R66F

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370401

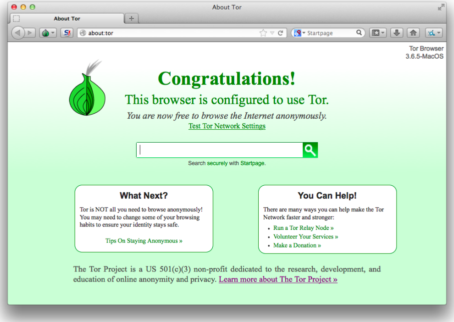
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
NATIONAL SECURITY AGENCY
SIGDEV
SIGINT DEVELOPMENT
SIGINT Development
MASTERSHAKE
SSG Governance and Enterprise Management

Al Jazeeras Islamabad bureau chief Ahmad Muaffaq Zaidan was labeled as a member of Al Qaeda by the NSA's metadata analysis.

"We kill people based on metadata"
- Michael Hayden (Ex-NSA Director)

Tor protects location metadata.
Tor Browser controls tracking when surfing the web.



Tor Browser
3.6.5-MacOS

Congratulations!

This browser is configured to use Tor.

*You are now free to browse the Internet anonymously.*

Test Tor Network Settings

Search securely with Startpage.

**What Next?**

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

**You Can Help!**

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

But what about the rest of the Internet?

# E-mail: Asynchronous messaging

- Email with GnuPG provides authenticity and confidentiality...

# E-mail: Asynchronous messaging

- Email with GnuPG provides authenticity and confidentiality...
- ... but fails to protect metadata
- ... and also fails to provide *forward secrecy* aka *key erasure*

# Why forward secrecy?

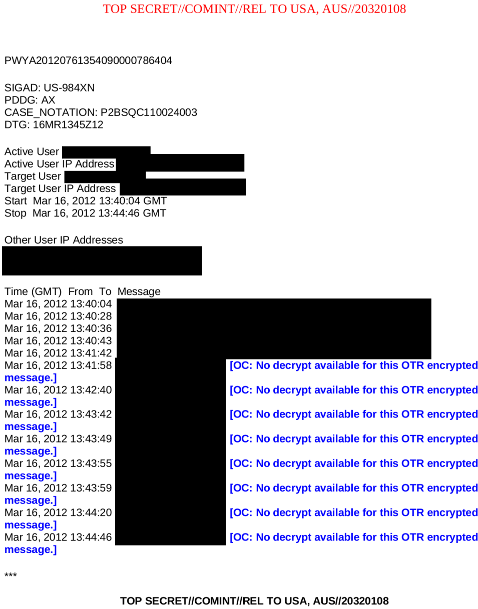
Imagine Eve records your GnuPG encrypted emails *now*, say here:

If Eve *ever* compromises your private key in the *future*, then she can read the encrypted emails you sent *today*.

# Synchronous messaging

## XMPP/OtR over Tor

- Forward secrecy from OtR
- User-friendly key exchange
- Location protection (Tor)
- ... but not asynchronous
- ... and leaks metadata
- No encrypted file transfers



TOP SECRET//COMINT//REL TO USA, AUS//20320108

PWYA20120761354090000786404

SIGAD: US-984XN
PDDG: AX
CASE_NOTATION: P2BSQC110024003
DTG: 16MR1345Z12

Active User [redacted]
Active User IP Address [redacted]
Target User [redacted]
Target User IP Address [redacted]
Start Mar 16, 2012 13:40:04 GMT
Stop Mar 16, 2012 13:44:46 GMT

Other User IP Addresses
[redacted]

```
Time (GMT)  From  To  Message
Mar 16, 2012 13:40:04 [redacted]
Mar 16, 2012 13:40:28
Mar 16, 2012 13:40:36
Mar 16, 2012 13:40:43
Mar 16, 2012 13:41:42
Mar 16, 2012 13:41:58 [redacted] [OC: No decrypt available for this OTR encrypted
message.]
Mar 16, 2012 13:42:40 [redacted] [OC: No decrypt available for this OTR encrypted
message.]
Mar 16, 2012 13:43:42 [redacted] [OC: No decrypt available for this OTR encrypted
message.]
Mar 16, 2012 13:43:49 [redacted] [OC: No decrypt available for this OTR encrypted
message.]
Mar 16, 2012 13:43:55 [redacted] [OC: No decrypt available for this OTR encrypted
message.]
Mar 16, 2012 13:43:59 [redacted] [OC: No decrypt available for this OTR encrypted
message.]
Mar 16, 2012 13:44:20 [redacted] [OC: No decrypt available for this OTR encrypted
message.]
Mar 16, 2012 13:44:46 [redacted] [OC: No decrypt available for this OTR encrypted
message.]
```

***

TOP SECRET//COMINT//REL TO USA, AUS//20320108

# Why is OtR synchronous only?

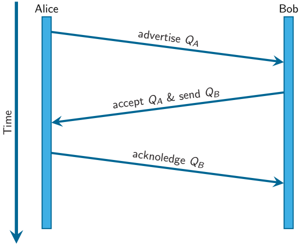
We achieve *forward secrecy* through *key erasure* by negotiating an ephemeral session key using Diffie-Hellman.

Diffie-Hellman key exchange uses commutativity of exponentiation:

$$A^b = (g^a)^b = (g^b)^a = B^a \bmod p$$

Elliptic curve Diffie-Hellman uses commutativity of scalar multiplication:

$$d_A Q_B = d_A d_B G = d_B d_A G = d_B Q_A$$



Private keys:
$d_A$, $d_B$

Public keys:
$Q_A = d_A G$
$Q_B = d_B G$

# Why is OtR synchronous only?

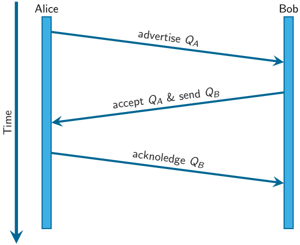
We achieve *forward secrecy* through *key erasure* by negotiating an ephemeral session key using Diffie-Hellman.

Diffie-Hellman key exchange uses commutativity of exponentiation:

$$A^b = (g^a)^b = (g^b)^a = B^a \bmod p$$

Elliptic curve Diffie-Hellman uses commutativity of scalar multiplication:

$$d_A Q_B = d_A d_B G = d_B d_A G = d_B Q_A$$



Private keys:
$d_A$, $d_B$

Public keys:
$Q_A = d_A G$
$Q_B = d_B G$

Answer: All three messages of the Diffie-Hellman key exchange must complete before OtR can use a new ratchet key.

# Axolotl by Trever Perin

Idea from Silence Circle's SCIMP:
Replace our key with its own hash.

Good: New key in zero round trips.

Bad: Stays compramized in future.

Approach:
Run DH whenever possible
Iterate key by hashing otherwise

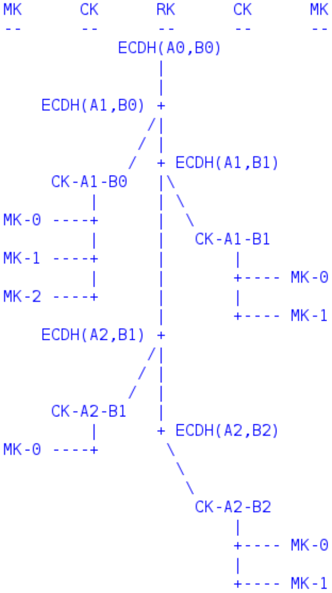
*"[Axolotl] combines the .. forward secrecy [of] a hash iteration ratchet like SCIMP [with the] future secrecy .. of a DH ratchet like OtR"* — *Moxie Marlenspike*

# Axolotl by Trever Perin

Approach:
 Run DH whenever possible
 Iterate key by hashing otherwise

Way less bookeeping!

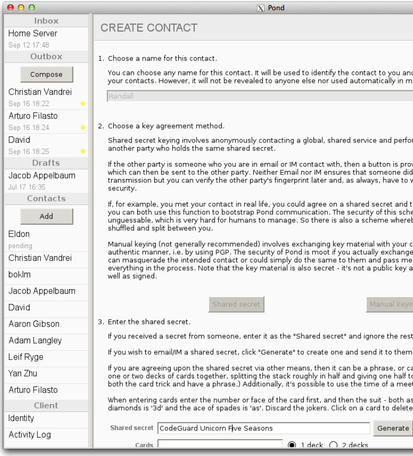
TripleDH provides authentication
 with deniability.



# Pond by Adam Langley

- Axolotl
- Recipients are pseudonynomous
- All traffic uses Tor
  with a constant traffic profile
- Senders are anonymous but
  authenticated by server
  not anonymous to the recipient
  No SPAM!
- Messages are deniable
- Encrypted attachments
- Forgets messages by default

https://pond.imperialviolet.org/



CREATE CONTACT

1. Choose a name for this contact.

You can choose any name for this contact. It will be used to identify the contact to you anc
your contacts. However, it will not be revealed to anyone else nor used automatically in m

Randall

2. Choose a key agreement method.

Shared secret keying involves anonymously contacting a global, shared service and perfor
another party who holds the same shared secret.

If the other party is someone who you are in email or IM contact with, then a button is prov
which can then be sent to the other party. Neither Email nor IM ensures that someone did
transmission but you can verify the other party's fingerprint later and, as always, have to w
security.

If, for example, you met your contact in real life, you could agree on a shared secret and t
you can both use this function to bootstrap Pond communication. The security of this sche
unguessable, which is very hard for humans to manage. So there is also a scheme whereb
shuffled and split between you.

Manual keying (not generally recommended) involves exchanging key material with your c
authentic manner, i.e. by using PGP. The security of Pond is moot if you actually exchange
can masquerade the intended contact or could simply do the same to them and pass me
everything in the process. Note that the key material is also secret - it's not a public key a
well as signed.

3. Enter the shared secret.

If you received a secret from someone, enter it as the "Shared secret" and ignore the rest

If you wish to email/IM a shared secret, click "Generate" to create one and send it to them

If you are agreeing upon the shared secret via other means, then it can be a phrase, or ca
one or two decks of cards together, splitting the stack roughly in half and giving one half to
both the card trick and have a phrase.) Additionally, it's possible to use the time of a meet

When entering cards enter the number or face of the card first, and then the suit - both as
diamonds is '3d' and the ace of spades is 'as'. Discard the jokers. Click on a card to delete

Shared secret: CodeGuard Unicorn Five Seasons

Cards: ● 1 deck ○ 2 decks

# End-to-end encrypted messengers

| | Syncronous | Asynchronous | Key Exchange | Key Erasure | Hides Location | Hides Metadata |
|---|---|---|---|---|---|---|
| Email + GnuPG | | ✓ | WoT | ✗ | ✗ | ✗ |
| XMPP + OtR | ✓ | | SMP | session | ✗ | ✗ |
| ... + Tor | | | X.509 | | ✓ | ✗ |
| TextSecure | ✓ | ✓ | TOFU | Axolotl | ✗ | ✗ |
| Pond | | ✓ | PANDA | Axolotl | Tor | ✓ |

Wot = Web of Trust

SMP = Socialist Millionare's Protocol

TOFU = Trust on first use

PANDA is a password authenticated key exchange system

# Key exchange and name systems

- Identify users (or servers) by name
- Associate names with addresses, key material and other properties
- DNS was the first global system to do this, insecurely
- X.509, DNSSEC, Web-of-Trust, TOFU, SMP, PANDA and Namecoin also operate in this domain

**NSA/CSS Threat Operations Center**

Cyber Profiling and Operations Support (V43)

# (U) MORECOWBELL

(S//REL) A Covert HTTP/ DNS Monitoring System for Operations Support

# Name System Properties

| | Suitable for personal use | Memorable | Decentralised | Modern cryptography | Understandable | Hides metadata | Transitive | Extensible |
|---|---|---|---|---|---|---|---|---|
| DNS | ❌ | ✓ | ❌ | ❌ | ✗ | ❌ | ✓ | ✗ |
| DNSSEC | ❌ | ✓ | ❌ | ❌ | ❌ | ❌ | ✓ | ✗ |
| TLS-X.509 | ❌ | ✓ | ✗ | ❌ | ❌ | ❌ | ✓ | ✗ |
| Web of Trust | ✓ | ✗ | ✓ | ✗ | ❌ | ❌ | ✓ | ✗ |
| TOFU | ✓ | ❌ | ✓ | | ✓ | ✓ | ❌ | ❌ |
| SMP/PANDA | ✓ | ❌ | ✓ | ✓ | ✓ | ✓ | ❌ | ❌ |
| Namecoin | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ |

# Name System Properties

| | Suitable for personal use | Memorable | Decentralised | Modern cryptography | Understandable | Hides metadata | Transitive | Extensible |
|---|---|---|---|---|---|---|---|---|
| DNS | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| DNSSEC | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| TLS-X.509 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Web of Trust | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ |
| TOFU | ✓ | ✗ | ✓ | | ✓ | ✓ | ✗ | ✗ |
| SMP/PANDA | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| Namecoin | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ |
| GNS | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

# The GNU Name System[1]

## Properties of GNS

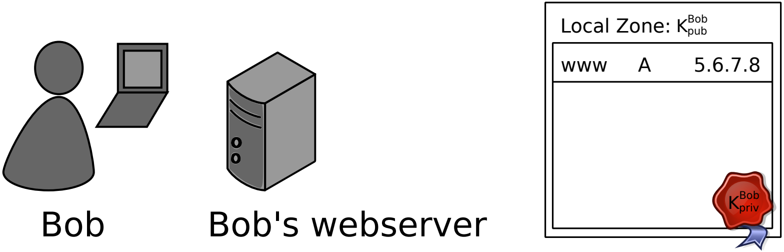
- Decentralized name system with secure memorable names
- Delegation used to achieve transitivity
- Supports globally unique, secure identifiers
- Achieves query and response privacy
- Provides alternative public key infrastructure
- Interoperable with DNS

## New applications enabled by GNS

- Name services hosted in P2P networks
- Name users in decentralized social networking applications

[1] Joint work with Martin Schanzenbach and Matthias Wachs

# Name resolution in GNS

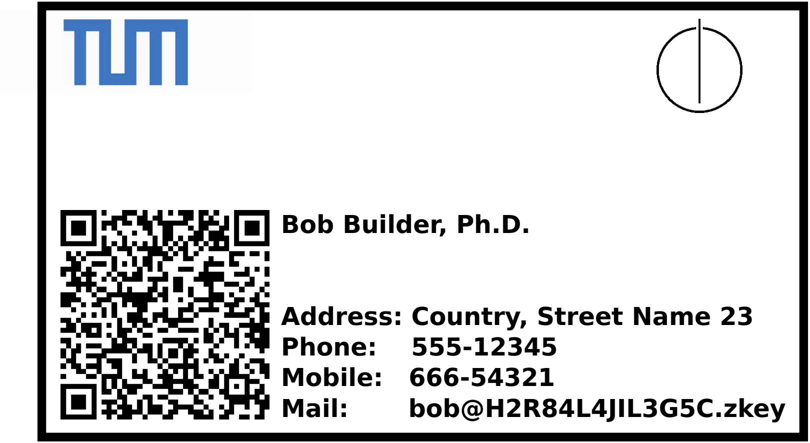


Local Zone: $K_{pub}^{Bob}$

| | | |
|---|---|---|
| www | A | 5.6.7.8 |

- Bob can locally reach his webserver via **www.gnu**

# Secure introduction

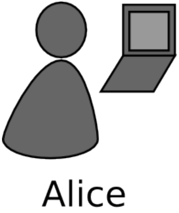


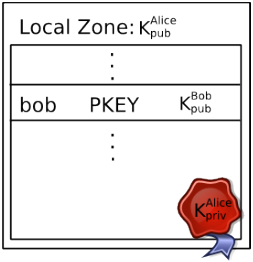
**Bob Builder, Ph.D.**

**Address: Country, Street Name 23**
**Phone: 555-12345**
**Mobile: 666-54321**
**Mail: bob@H2R84L4JIL3G5C.zkey**

- Bob gives his public key to his **friends**, possibly via QR code

# Delegation





Local Zone: $K_{pub}^{Alice}$

⋮

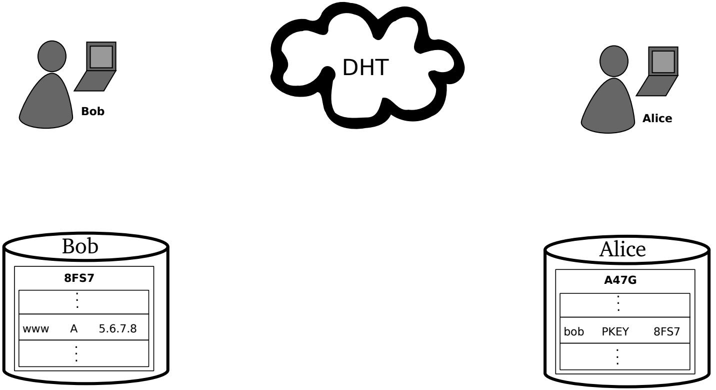
bob PKEY $K_{pub}^{Bob}$

⋮

$K_{priv}^{Alice}$

- Alice learns Bob's public key
- Alice creates delegation to zone $K_{pub}^{Bob}$ under label **bob**
- Alice can reach Bob's webserver via **www.bob.gnu**

# Name Resolution



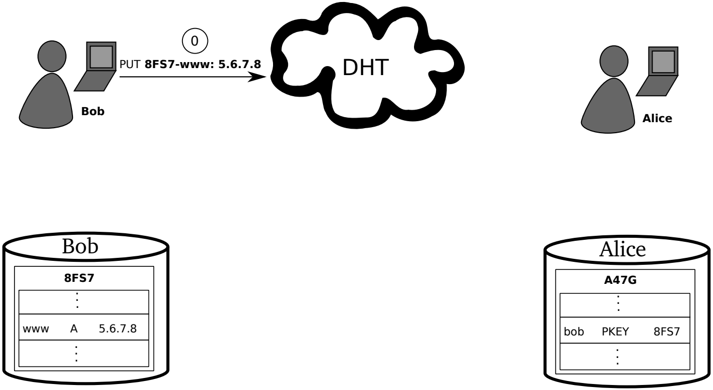
Bob

| 8FS7 | | |
|---|---|---|
| | ⋮ | |
| www | A | 5.6.7.8 |
| | ⋮ | |

Alice

| A47G | | |
|---|---|---|
| | ⋮ | |
| bob | PKEY | 8FS7 |
| | ⋮ | |

# Name Resolution



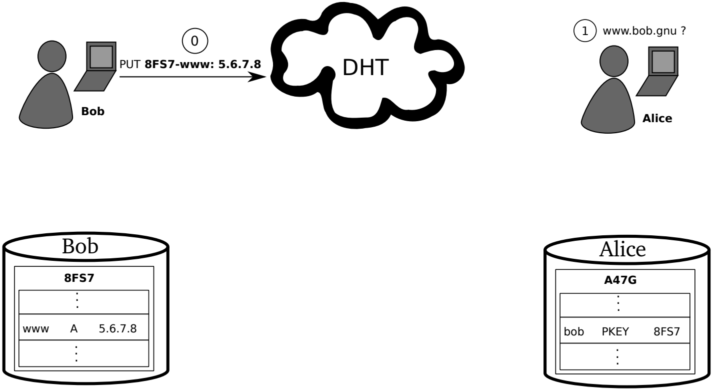
**8FS7**

| | | |
|---|---|---|
| ⋮ | | |
| www | A | 5.6.7.8 |
| ⋮ | | |

**A47G**

| | | |
|---|---|---|
| ⋮ | | |
| bob | PKEY | 8FS7 |
| ⋮ | | |

# Name Resolution



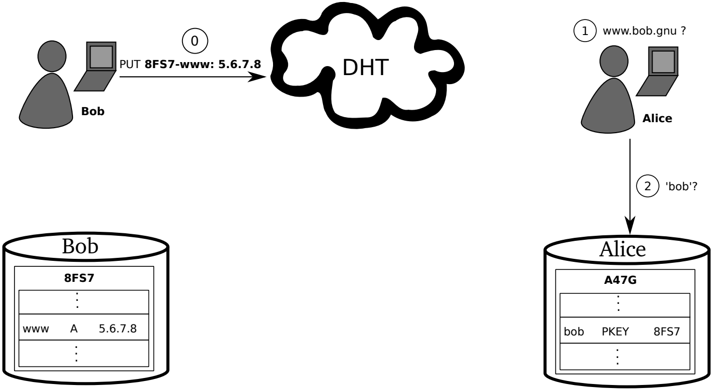
Bob

| **8FS7** | | |
|---|---|---|
| | ⋮ | |
| www | A | 5.6.7.8 |
| | ⋮ | |

Alice

| **A47G** | | |
|---|---|---|
| | ⋮ | |
| bob | PKEY | 8FS7 |
| | ⋮ | |

# Name Resolution



**8FS7**

⋮

www A 5.6.7.8

⋮

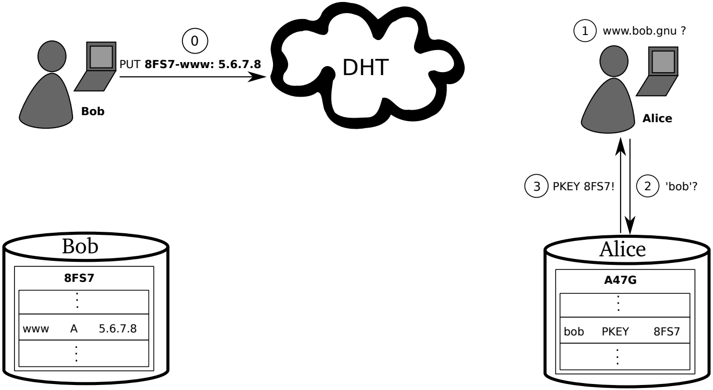
**A47G**

⋮

bob PKEY 8FS7

⋮

# Name Resolution



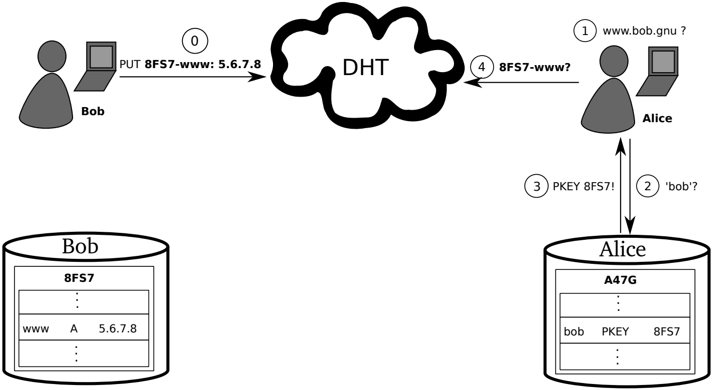
**8FS7**

|     |     |     |
|-----|-----|-----|
|     | ⋮   |     |
| www | A   | 5.6.7.8 |
|     | ⋮   |     |

**A47G**

|     |      |      |
|-----|------|------|
|     | ⋮    |      |
| bob | PKEY | 8FS7 |
|     | ⋮    |      |

# Name Resolution



**8FS7**

⋮

www A 5.6.7.8

⋮

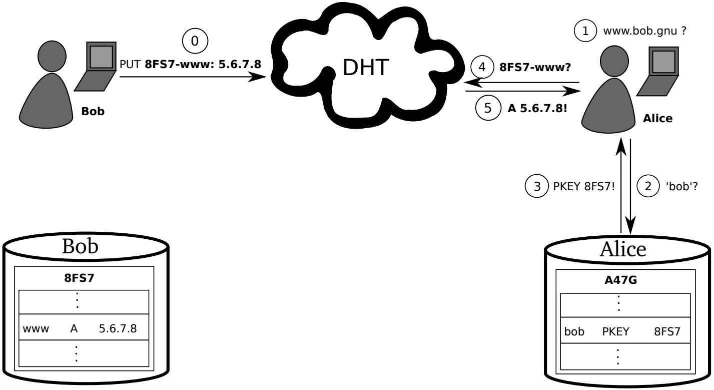
**A47G**

⋮

bob PKEY 8FS7

⋮

# Name Resolution



# Query Privacy: Terminology

$G$ generator in ECC curve, a point

$n$ size of ECC group, $n := |G|$, $n$ prime

$x$ private ECC key of zone ($x \in \mathbb{Z}_n$)

$P$ public key of zone, a point $P := xG$

$l$ label for record in a zone ($l \in \mathbb{Z}_n$)

$R_{P,l}$ set of records for label $l$ in zone $P$

$q_{P,l}$ query hash (hash code for DHT lookup)

$B_{P,l}$ block with encrypted information for label $l$ in zone $P$ published in the DHT under $q_{P,l}$

# Query Privacy: Cryptography

## Publishing records $R_{P,l}$ as $B_{P,l}$ under key $q_{P,l}$

$$
\begin{aligned}
h &:= H(l, P) && (1)\\
d &:= h \cdot x \mod n && (2)\\
B_{P,l} &:= S_d(E_{HKDF(l,P)}(R_{P,l})), dG && (3)\\
q_{P,l} &:= H(dG) && (4)
\end{aligned}
$$

# Query Privacy: Cryptography

## Publishing records $R_{P,l}$ as $B_{P,l}$ under key $q_{P,l}$

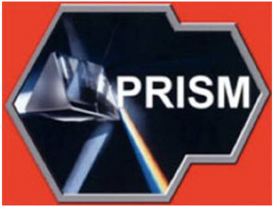
$$\begin{aligned} h &:= H(l, P) && (1) \\ d &:= h \cdot x \mod n && (2) \\ B_{P,l} &:= S_d(E_{HKDF(l,P)}(R_{P,l})), dG && (3) \\ q_{P,l} &:= H(dG) && (4) \end{aligned}$$

## Searching for records under label $l$ in zone $P$

$$\begin{aligned} h &:= H(l, P) && (5) \\ q_{P,l} &:= H(hP) = H(hxG) = H(dG) \Rightarrow \texttt{obtain } B_{P,l} && (6) \\ R_{P,l} &= D_{HKDF(l,P)}(B_{P,l}) && (7) \end{aligned}$$

Is this it?

Is this it?

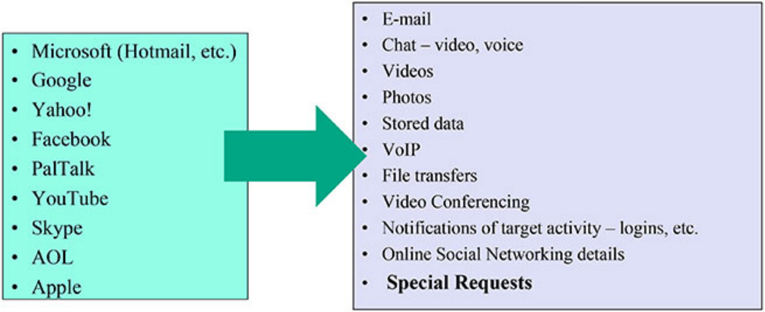


Gmail facebook Hotmail YAHOO! Google skype paltalk.com YouTube AOL mail

SPECIAL SOURCE OPERATIONS

# (TS//SI//NF) PRISM Collection Details

PRISM



Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

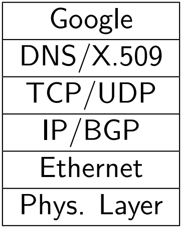
- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

# Sometime in 2013...

# The ~~NEW~~GNU Network (very simplified)

*Internet*



Google

DNS/X.509

TCP/UDP

IP/BGP

Ethernet

Phys. Layer

# The ~~NEW~~GNU Network (very simplified)

| *Internet* | |
|---|---|
| Google | |
| DNS/X.509 | |
| TCP/UDP | |
| IP/BGP | |
| Ethernet | |
| Phys. Layer | HTTPS/TCP/WLAN/... |

# The ~~NEW~~GNU Network (very simplified)

*Internet*

| |
|---|
| Google |
| DNS/X.509 |
| TCP/UDP |
| IP/BGP |
| Ethernet |
| Phys. Layer |

| |
|---|
| |
| |
| |
| |
| CORE (OTR) |
| HTTPS/TCP/WLAN/... |

# The ~~NEW~~GNU Network (very simplified)

| *Internet* | |
|---|---|
| Google | |
| DNS/X.509 | |
| TCP/UDP | |
| IP/BGP | $R^5N$ DHT |
| Ethernet | CORE (OTR) |
| Phys. Layer | HTTPS/TCP/WLAN/... |

# The ~~NEW~~GNU Network (very simplified)

| *Internet* | |
|---|---|
| Google | |
| DNS/X.509 | |
| TCP/UDP | CADET (AXOLOTL) |
| IP/BGP | $R^5N$ DHT |
| Ethernet | CORE (OTR) |
| Phys. Layer | HTTPS/TCP/WLAN/... |

# The ~~NEW~~GNU Network (very simplified)

| *Internet* | |
|---|---|
| Google | |
| DNS/X.509 | GNU Name System |
| TCP/UDP | CADET (AXOLOTL) |
| IP/BGP | $R^5N$ DHT |
| Ethernet | CORE (OTR) |
| Phys. Layer | HTTPS/TCP/WLAN/... |

# The ~~NEW~~GNU Network (very simplified)

| *Internet* | |
|---|---|
| Google | Applications |
| DNS/X.509 | GNU Name System |
| TCP/UDP | CADET (AXOLOTL) |
| IP/BGP | $R^5N$ DHT |
| Ethernet | CORE (OTR) |
| Phys. Layer | HTTPS/TCP/WLAN/... |

# The ~~NEW~~GNU Network (very simplified)

| *Internet* | *GNUnet* |
|---|---|
| Google | Applications |
| DNS/X.509 | GNU Name System |
| TCP/UDP | CADET (AXOLOTL) |
| IP/BGP | $R^5N$ DHT |
| Ethernet | CORE (OTR) |
| Phys. Layer | HTTPS/TCP/WLAN/... |

# Applications?

- Anonymous file-sharing
- Conversation
- Electronic voting (WiP)
- Messaging (WiP)
- News distribution (WiP)
- Social networking (WiP)

# Applications?

- Anonymous file-sharing
- Conversation
- Electronic voting (WiP)
- Messaging (WiP)
- News distribution (WiP)
- Social networking (WiP)
- Payment (WiP)

# GNU Taler

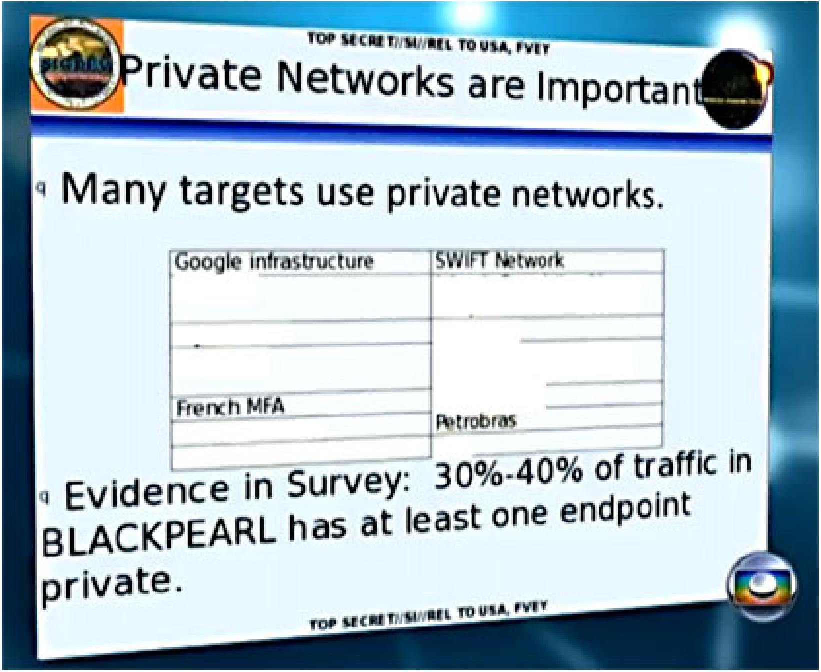
**Modern economies need a currency.**

# Motivation

**Modern economies need a currency online.**

# SWIFT?

**SWIFT/Mastercard/Visa are too transparent.**



# Private Networks are Important

- Many targets use private networks.

| Google infrastructure | SWIFT Network |
|---|---|
| | |
| | |
| French MFA | Petrobras |
| | |

- Evidence in Survey: 30%-40% of traffic in BLACKPEARL has at least one endpoint private.

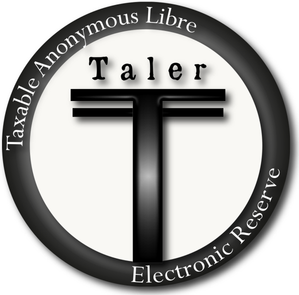
This was a question posed to RAND researchers in 1971:

> *"Suppose you were an advisor to the head of the KGB, the Soviet Secret Police. Suppose you are given the assignment of designing a system for the surveillance of all citizens and visitors within the boundaries of the USSR. The system is not to be too obtrusive or obvious. What would be your decision?"*

The result: an electronic funds transfer system that looks strikingly similar today's debit card system.

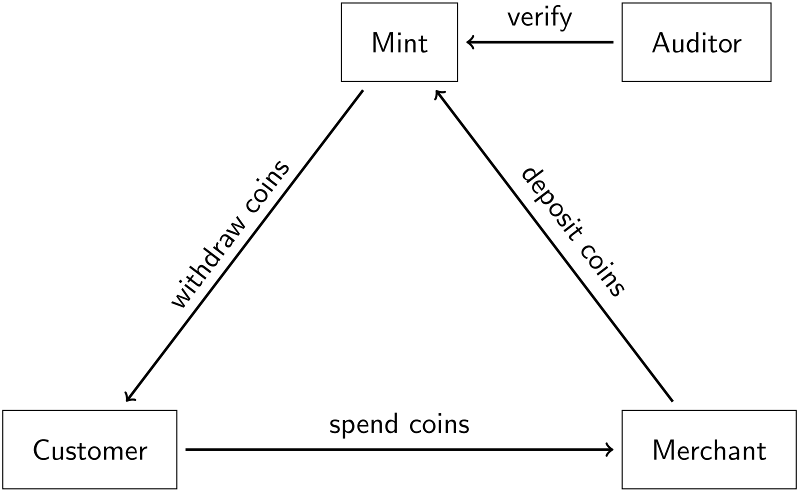
# Let's make cash **digital** and **socially responsible**.

# Let's make cash **digital** and **socially responsible**.



Taxable, Anonymous, Libre, Practical, Resource Friendly

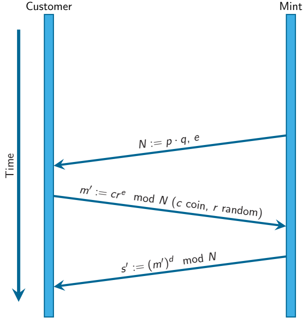
# Architecture of GNU Taler



# Blind Signatures (Chaum)

Mint picks primes $p$ and $q$, random $e$ and a $d$ such that:

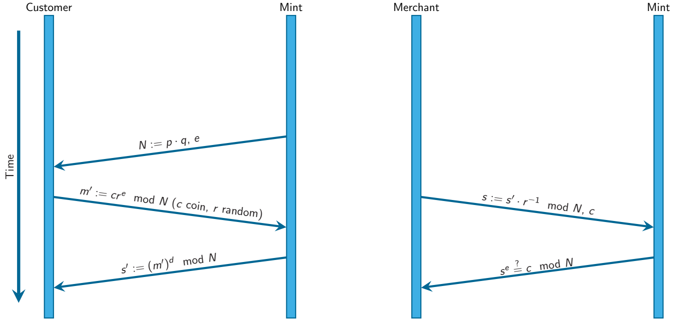
$$de \equiv 1 \mod (p-1)(q-1) \tag{8}$$



# Blind Signatures (Chaum)

Mint picks primes $p$ and $q$, random $e$ and a $d$ such that:

$$de \equiv 1 \mod (p-1)(q-1) \tag{8}$$



Customer
Mint
Merchant
Mint
Time
$N := p \cdot q,\ e$
$m' := cr^e \mod N$ ($c$ coin, $r$ random)
$s' := (m')^d \mod N$
$s := s' \cdot r^{-1} \mod N,\ c$
$s^e \overset{?}{=} c \mod N$

# Questions? Answers!

- `http://www.decentralise.rennes.inria.fr/`
- `https://gnunet.org/videos`
- `http://www.taler.net/`
- `https://pond.imperialviolet.org/`